

Vault 7: Projects



This publication series is about specific projects related to the [Vault 7](#) main publication.

[Releases ▼](#)[Documents ▼](#)

All Releases

[Protego](#) - 7 September, 2017[Angelfire](#) - 31 August, 2017[ExpressLane](#) - 24 August, 2017[CouchPotato](#) - 10 August, 2017[Dumbo](#) - 3 August, 2017[Imperial](#) - 27 July, 2017[UCL / Raytheon](#) - 19 July, 2017[Highrise](#) - 13 July, 2017[BothanSpy](#) - 6 July, 2017[OutlawCountry](#) - 30 June, 2017[Elsa](#) - 28 June, 2017[Brutal Kangaroo](#) - 22 June, 2017[Cherry Blossom](#) - 15 June, 2017[Pandemic](#) - 1 June, 2017[Athena](#) - 19 May, 2017[AfterMidnight](#) - 12 May, 2017[Archimedes](#) - 5 May, 2017[Scribbles](#) - 28 April, 2017[Weeping Angel](#) - 21 April, 2017

Protego

7 September, 2017

Today, September 7th 2017, WikiLeaks publishes four secret documents from the *Protego* project of the CIA, along with 37 related documents (proprietary hardware/software manuals from [Microchip Technology Inc.](#)). The project was maintained between 2014 and 2015.

Protego is not the "usual" malware development project like all previous publications by WikiLeaks in the [Vault7 series](#). Indeed there is no explicit indication why it is part of the project repositories of the CIA/EDG at all.

The *Protego* project is a [PIC](#)-based missile control system that was developed by [Raytheon](#). The documents indicate that the system is installed on-board a [Pratt & Whitney](#) aircraft (PWA) equipped with missile launch systems (air-to-air and/or air-to-ground).

Protego consists of separate micro-controller units that exchange data and signals over encrypted and authenticated channels:

» On-board TWA are the 'Master Processor' (MP) and the 'Deployment Box'. Both systems are layed-out with master/slave redundancy.

» The missile system has micro-controllers for the missile itself ('Missile Smart Switch', MSS), the tube ('Tube Smart Switch', TSS) and the collar (which holds the missile before and at launch time).

The MP unit receives three signals from a beacon: 'In Border' (PWA is within the defined area of an operation), 'Valid GPS' (GPS signal available) and 'No End of Operational Period' (current time is within the defined timeframe for an operation). Missiles can only be launched if all signals received by MP are set to 'true'. Similary safeguards are in place to auto-destruct encryption and authentication keys for various scenarios (like 'leaving a target area of operation' or 'missing missile').

Leaked Documents



[Protego Release 01.05](#)
-- System HW
Description



[Protego Release 01.05](#)
-- Build Procedure



[Protego Release 01.05](#)
-- Message Format



[Protego Release 01.05](#)
-- SW SCRs

Today, August 31st 2017, WikiLeaks publishes documents from the *Angelfire* project of the CIA. *Angelfire* is an implant comprised of five components: Solartime, *Wolfcreek*, Keystone (previously MagicWand), *BadMFS*, and the Windows Transitory File system. Like previously published CIA projects ([Grasshopper](#) and [AfterMidnight](#)) in the [Vault7 series](#), it is a persistent framework that can load and execute custom implants on target computers running the Microsoft Windows operating system (XP or Win7).

Solartime modifies the partition boot sector so that when Windows loads boot time device drivers, it also loads and executes the *Wolfcreek* implant, that once executed, can load and run other *Angelfire* implants. According to the documents, the loading of additional implants creates memory leaks that can be possibly detected on infected machines.

Keystone is part of the *Wolfcreek* implant and responsible for starting malicious user applications. Loaded implants never touch the file system, so there is very little forensic evidence that the process was ever ran. It always disguises as "C:\Windows\system32\svchost.exe" and can thus be detected in the Windows task manager, if the operating system is installed on another partition or in a different path.

BadMFS is a library that implements a covert file system that is created at the end of the active partition (or in a file on disk in later versions). It is used to store all drivers and implants that *Wolfcreek* will start. All files are both encrypted and obfuscated to avoid string or PE header scanning. Some versions of *BadMFS* can be detected because the reference to the covert file system is stored in a file named "zf".

The Windows Transitory File system is the new method of installing *AngelFire*. Rather than lay independent components on disk, the system allows an operator to create transitory files for specific actions including installation, adding files to *AngelFire*, removing files from *AngelFire*, etc. Transitory files are added to the 'UserInstallApp'.

Leaked Documents

[Angelfire 2.0 -- User Guide](#)[BadMFS -- Developer Guide](#)[Wolfcreek Docs -- Angelfire User Guide](#)[Wolfcreek Docs -- Angelfire Test Matrix](#)[Wolfcreek Docs -- Notes](#)[See more](#)

among many others the National Security Agency (NSA), the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI).

The OTS ([Office of Technical Services](#)), a branch within the CIA, has a biometric collection system that is provided to liaison services around the world -- with the expectation for sharing of the biometric takes collected on the systems. But this 'voluntary sharing' obviously does not work or is considered insufficient by the CIA, because *ExpressLane* is a covert information collection tool that is used by the CIA to secretly exfiltrate data collections from such systems provided to liaison services.

ExpressLane is installed and run with the cover of upgrading the biometric software by OTS agents that visit the liaison sites. Liaison officers overseeing this procedure will remain unsuspecting, as the data exfiltration disguises behind a Windows installation splash screen.

The core components of the OTS system are based on products from [Cross Match](#), a US company specializing in biometric software for law enforcement and the Intelligence Community. The company hit the headlines in 2011 when it was reported that the US military [used a Cross Match product to identify Osama bin Laden](#) during the assassination operation in Pakistan.

CouchPotato


10 August, 2017

Today, August 10th 2017, WikiLeaks publishes the the User Guide for the *CoachPotato* project of the CIA. *CouchPotato* is a remote tool for collection against RTSP/H.264 video streams. It provides the ability to collect either the stream as a video file (AVI) or capture still images (JPG) of frames from the stream that are of significant change from a previously captured frame. It utilizes ffmpeg for video and image encoding and decoding as well as RTSP connectivity. *CouchPotato* relies on being launched in an ICE v3 Fire and Collect compatible loader.

 [Tool Delivery Review](#)

 [ExpressLane v3.1.1 -- TPP FINAL](#)

 [ExpressLane v3.1.1 -- User Manual](#)

 [ExpressLane v3.1.1 -- Requirement Statement](#)

 [ExpressLane v3.0 -- User Guide](#)

[See more](#)

Leaked Documents



 [CouchPotato v1.0 -- User Guide](#)

Today, August 3rd 2017 WikiLeaks publishes documents from the *Dumbo* project of the CIA. *Dumbo* is a capability to suspend processes utilizing webcams and corrupt any video recordings that could compromise a PAG deployment. The PAG (Physical Access Group) is a special branch within the CCI (Center for Cyber Intelligence); its task is to gain and exploit physical access to target computers in CIA field operations.

Dumbo can identify, control and manipulate monitoring and detection systems on a target computer running the Microsoft Windows operating system. It identifies installed devices like webcams and microphones, either locally or connected by wireless (Bluetooth, WiFi) or wired networks. All processes related to the detected devices (usually recording, monitoring or detection of video/audio/network streams) are also identified and can be stopped by the operator. By deleting or manipulating recordings the operator is aided in creating fake or destroying actual evidence of the intrusion operation.

Dumbo is run by the field agent directly from an USB stick; it requires administrator privileges to perform its task. It supports 32bit Windows XP, Windows Vista, and newer versions of Windows operating system. 64bit Windows XP, or Windows versions prior to XP are not supported.

Leaked Documents

-  [Dumbo v3.0 -- Field Guide](#)
-  [Dumbo v3.0 -- User Guide](#)
-  [Dumbo v2.0 -- Field Guide](#)
-  [Dumbo v2.0 -- User Guide](#)
-  [Dumbo v1.0 -- TDR Briefing](#)

[See more](#)

Imperial

27 July, 2017

Today, July 27th 2017, WikiLeaks publishes documents from the *Imperial* project of the CIA.

Achilles is a capability that provides an operator the ability to trojan an OS X disk image (.dmg) installer with one or more desired operator specified executables for a one-time execution.

Aeris is an automated implant written in C that supports a number of POSIX-based systems (Debian, RHEL, Solaris, FreeBSD, CentOS). It supports automated file exfiltration, configurable beacon interval and jitter, standalone and Collide-based HTTPS LP support and SMTP protocol

Leaked Documents

-  [Achilles -- User Guide](#)
-  [SeaPea -- User Guide](#)
-  [Aeris -- Users Guide](#)

SeaPea is an OS X Rootkit that provides stealth and tool launching capabilities. It hides files/directories, socket connections and/or processes. It runs on Mac OSX 10.6 and 10.7.

UCL / Raytheon

19 July, 2017

Today, July 19th 2017, WikiLeaks publishes documents from the CIA contractor *Raytheon Blackbird Technologies* for the "[UMBRAGE Component Library](#)" (UCL) project. The documents were submitted to the CIA between November 21st, 2014 (just two weeks after [Raytheon acquired Blackbird Technologies](#) to build a [Cyber Powerhouse](#)) and September 11th, 2015. They mostly contain Proof-of-Concept ideas and assessments for malware attack vectors - partly based on public documents from security researchers and private enterprises in the computer security field.

Raytheon Blackbird Technologies acted as a kind of "technology scout" for the [Remote Development Branch \(RDB\)](#) of the CIA by analysing malware attacks in the wild and giving recommendations to the CIA development teams for further investigation and PoC development for their own malware projects.

Leaked Documents



(S//NF) CSIT 15083 -- HTTPBrowser



(S//NF) CSIT 15085 -- NfLog



(S//NF) Symantec -- Regin - Stealthy Surveillance



(S//NF) FireEye -- HammerToss - Stealthy Tactics



(S//NF) VB -- Gamker

[See more](#)

Highrise

13 July, 2017

Today, July 13th 2017, WikiLeaks publishes documents from the *Highrise* project of the CIA. *HighRise* is an Android application designed for mobile devices running Android 4.0 to 4.3. It provides a redirector function for SMS messaging that could be used by a number of IOC tools that use SMS messages for communication between implants and listening posts. *HighRise* acts as a SMS proxy that provides greater separation between

Leaked Documents



HighRise 2.0 Users Guide

BothanSpy

6 July, 2017

Today, July 6th 2017, WikiLeaks publishes documents from the *BothanSpy* and *Gyrfalcon* projects of the CIA. The implants described in both projects are designed to intercept and exfiltrate SSH credentials but work on different operating systems with different attack vectors.

BothanSpy is an implant that targets the SSH client program Xshell on the Microsoft Windows platform and steals user credentials for all active SSH sessions. These credentials are either username and password in case of password-authenticated SSH sessions or username, filename of private SSH key and key password if public key authentication is used.

BothanSpy can exfiltrate the stolen credentials to a CIA-controlled server (so the implant never touches the disk on the target system) or save it in an encrypted file for later exfiltration by other means. *BothanSpy* is installed as a Shellterm 3.x extension on the target machine.

Gyrfalcon is an implant that targets the OpenSSH client on Linux platforms (centos,debian,rhel,suse,ubuntu). The implant can not only steal user credentials of active SSH sessions, but is also capable of collecting full or partial OpenSSH session traffic. All collected information is stored in an encrypted file for later exfiltration. It is installed and configured by using a CIA-developed root kit (JQC/KitV) on the target machine.

OutlawCountry

30 June, 2017

Today, June 30th 2017, WikiLeaks publishes documents from the *OutlawCountry* project of the CIA that targets computers running the Linux operating system. *OutlawCountry* allows for the redirection of all outbound network traffic on the target computer to CIA controlled machines for ex- and infiltration purposes. The malware consists of a kernel module that creates a hidden netfilter table on a Linux target; with knowledge of the

Leaked Documents



[BothanSpy 1.0](#)



[Gyrfalcon 2.0 User Guide](#)



[Gyrfalcon 1.0 User Manual](#)

Leaked Documents



[OutlawCountry v1.0 User Manual](#)



[OutlawCountry v1.0 Test Plan](#)

detail in the document; an operator will have to rely on the available CIA exploits and backdoors to inject the kernel module into a target operating system. *OutlawCountry* v1.0 contains one kernel module for 64-bit CentOS/RHEL 6.x; this module will only work with default kernels. Also, *OutlawCountry* v1.0 only supports adding covert DNAT rules to the PREROUTING chain.

Elsa

28 June, 2017

Today, June 28th 2017, WikiLeaks publishes documents from the *ELSA* project of the CIA. *ELSA* is a geo-location malware for WiFi-enabled devices like laptops running the Microsoft Windows operating system. Once persistently installed on a target machine using separate CIA exploits, the malware scans visible WiFi access points and records the ESS identifier, MAC address and signal strength at regular intervals. To perform the data collection the target machine does not have to be online or connected to an access point; it only needs to be running with an enabled WiFi device. If it is connected to the internet, the malware automatically tries to use public geo-location databases from Google or Microsoft to resolve the position of the device and stores the longitude and latitude data along with the timestamp. The collected access point/geo-location information is stored in encrypted form on the device for later exfiltration. The malware itself does not beacon this data to a CIA back-end; instead the operator must actively retrieve the log file from the device - again using separate CIA exploits and backdoors.

The *ELSA* project allows the customization of the implant to match the target environment and operational objectives like sampling interval, maximum size of the logfile and invocation/persistence method. Additional back-end software (again using public geo-location databases from Google and Microsoft) converts unprocessed access point information from exfiltrated logfiles to geo-location data to create a tracking profile of the target device.

Leaked Documents



[ELSA User Manual](#)

Today, June 22nd 2017, WikiLeaks publishes documents from the *Brutal Kangaroo* project of the CIA. *Brutal Kangaroo* is a tool suite for Microsoft Windows that targets closed networks by air gap jumping using thumbdrives. *Brutal Kangaroo* components create a custom covert network within the target closed network and providing functionality for executing surveys, directory listings, and arbitrary executables.

The documents describe how a CIA operation can infiltrate a closed network (or a single air-gapped computer) within an organization or enterprise without direct access. It first infects a Internet-connected computer within the organization (referred to as "primary host") and installs the *BrutalKangeroo* malware on it. When a user is using the primary host and inserts a USB stick into it, the thumbdrive itself is infected with a separate malware. If this thumbdrive is used to copy data between the closed network and the LAN/WAN, the user will sooner or later plug the USB disk into a computer on the closed network. By browsing the USB drive with Windows Explorer on such a protected computer, it also gets infected with exfiltration/survey malware. If multiple computers on the closed network are under CIA control, they form a covert network to coordinate tasks and data exchange. Although not explicitly stated in the documents, this method of compromising closed networks is very similar to how [Stuxnet](#) worked.

The *Brutal Kangaroo* project consists of the following components: *Drifting Deadline* is the thumbdrive infection tool, *Shattered Assurance* is a server tool that handles automated infection of thumbdrives (as the primary mode of propagation for the *Brutal Kangaroo* suite), *Broken Promise* is the *Brutal Kangaroo* postprocessor (to evaluate collected information) and *Shadow* is the primary persistence mechanism (a stage 2 tool that is distributed across a closed network and acts as a covert command-and-control network; once multiple *Shadow* instances are installed and share drives, tasking and payloads can be sent back-and-forth).

The primary execution vector used by infected thumbdrives is a vulnerability in the Microsoft Windows operating system that can be exploited by hand-crafted link files that load and execute programs (DLLs)

Leaked Documents



[Brutal Kangaroo -- Drifting Deadline v1.2 - User Guide](#)



[EzCheese v6.3 - User Guide](#)



[EzCheese v6.2 - User Guide \(Rev. B\)](#)



[EzCheese v6.2 - User Guide \(Rev. A\)](#)



[EZCheese v6.2 - IVV TDR Slides](#)

[See more](#)

system.

Cherry Blossom

15 June, 2017

Today, June 15th 2017, WikiLeaks publishes documents from the *CherryBlossom* project of the CIA that was developed and implemented with the help of the US nonprofit [Stanford Research Institute \(SRI International\)](#).

CherryBlossom provides a means of monitoring the Internet activity of and performing software exploits on *Targets* of interest. In particular, *CherryBlossom* is focused on compromising wireless networking devices, such as wireless routers and access points (APs), to achieve these goals. Such Wi-Fi devices are commonly used as part of the Internet infrastructure in private homes, public spaces (bars, hotels or airports), small and medium sized companies as well as enterprise offices. Therefore these devices are the ideal spot for "Man-In-The-Middle" attacks, as they can easily monitor, control and manipulate the Internet traffic of connected users. By altering the data stream between the user and Internet services, the infected device can inject malicious content into the stream to exploit vulnerabilities in applications or the operating system on the computer of the targeted user.

The wireless device itself is compromised by implanting a customized *CherryBlossom* firmware on it; some devices allow upgrading their firmware over a wireless link, so no physical access to the device is necessary for a successful infection. Once the new firmware on the device is flashed, the router or access point will become a so-called *FlyTrap*. A *FlyTrap* will beacon over the Internet to a Command & Control server referred to as the *CherryTree*. The beacons information contains device status and security information that the *CherryTree* logs to a database. In response to this information, the *CherryTree* sends a *Mission* with operator-defined tasking. An operator can use *CherryWeb*, a browser-based user interface to view *Flytrap* status and security info, plan *Mission*

Leaked Documents

-  [CherryBlossom -- System Req Spec \(CDRL-10\)](#)
-  [CherryBlossom -- Quick Start Guide](#)
-  [WiFi Devices](#)
-  [CherryBlossom -- Installation Guide](#)
-  [CherryBlossom -- Operating Environment \(S//NF\)](#)

[See more](#)

beacon. Tasks for a *Flytrap* include (among others) the scan for *email addresses*, *chat usernames*, *MAC addresses* and *VoIP numbers* in passing network traffic to trigger additional actions, the copying of the full network traffic of a *Target*, the redirection of a *Target*'s browser (e.g., to Windex for browser exploitation) or the proxying of a *Target*'s network connections. *FlyTrap* can also setup VPN tunnels to a *CherryBlossom*-owned VPN server to give an operator access to clients on the *Flytrap*'s WLAN/LAN for further exploitation. When the *Flytrap* detects a *Target*, it will send an *Alert* to the *CherryTree* and commence any actions/exploits against the *Target*. The *CherryTree* logs *Alerts* to a database, and, potentially distributes *Alert* information to interested parties (via *Catapult*).

Pandemic

1 June, 2017

Today, June 1st 2017, WikiLeaks publishes documents from the "Pandemic" project of the CIA, a persistent implant for Microsoft Windows machines that share files (programs) with remote users in a local network. "Pandemic" targets remote users by replacing application code on-the-fly with a trojaned version if the program is retrieved from the infected machine. To obfuscate its activity, the original file on the file server remains unchanged; it is only modified/replaced while in transit from the pandemic file server before being executed on the computer of the remote user. The implant allows the replacement of up to 20 programs with a maximum size of 800 MB for a selected list of remote users (targets).

As the name suggests, a single computer on a local network with shared drives that is infected with the "Pandemic" implant will act like a "Patient Zero" in the spread of a disease. It will infect remote computers if the user executes programs stored on the pandemic file server. Although not explicitly stated in the documents, it seems technically feasible that remote computers that provide file shares themselves become new pandemic file servers on the local network to reach new targets.

Leaked Documents



[Pandemic 1.1 \(S/NF\)](#)



[Pandemic 1.1-RC1 \(S/NF\)](#)



[Pandemic 1.1-RC1 -- IVVRR Checklist](#)



[Pandemic 1.0 \(S/NF\)](#)



[Pandemic 1.0 -- IVVRR Checklist](#)

[See more](#)

Today, May 19th 2017, WikiLeaks publishes documents from the "Athena" project of the CIA. "Athena" - like the related "Hera" system - provides remote beacon and loader capabilities on target computers running the Microsoft Windows operating system (from Windows XP to Windows 10). Once installed, the malware provides a beaconing capability (including configuration and task handling), the memory loading/unloading of malicious payloads for specific tasks and the delivery and retrieval of files to/from a specified directory on the target system. It allows the operator to configure settings during runtime (while the implant is on target) to customize it to an operation.

According to the documentation (see [Athena Technology Overview](#)), the malware was developed by the CIA in cooperation with [Siege Technologies](#), a self-proclaimed cyber security company based in New Hampshire, US. On their website, Siege Technologies states that the company "... focuses on leveraging **offensive cyberwar technologies** and methodologies to develop predictive cyber security solutions for insurance, government and other targeted markets.". On November 15th, 2016 [Nehemiah Security](#) announced the acquisition of Siege Technologies.

In an email from HackingTeam (published by WikiLeaks [here](#)), Jason Syversen, founder of Siege Technologies with a background in cryptography and hacking, "... said he set out to create the equivalent of the military's so-called probability of kill metric, a statistical analysis of whether an attack is likely to succeed. 'I feel more comfortable working on electronic warfare,' he said. 'It's a little different than bombs and nuclear weapons -- that's a morally complex field to be in. Now instead of bombing things and having collateral damage, you can really reduce civilian casualties, which is a win for everybody.'"

Leaked Documents

[Athena v1.0 User Guide](#)[Athena Technology Overview](#)[Athena \(Design\)](#)[Athena \(Demo\)](#)[Athena \(Design/Engine\)](#)[See more](#)

AfterMidnight

12 May, 2017

"AfterMidnight" allows operators to dynamically load and execute malware payloads on a target machine. The main controller disguises as a self-persisting Windows Service DLL and provides secure execution of "Gremlins" via a HTTPS based Listening Post (LP) system called "Octopus". Once installed on a target machine AM will call back to a configured LP on a configurable schedule, checking to see if there is a new plan for it to execute. If there is, it downloads and stores all needed components before loading all new gremlins in memory. "Gremlins" are small AM payloads that are meant to run hidden on the target and either subvert the functionality of targeted software, survey the target (including data exfiltration) or provide internal services for other gremlins. The special payload "AlphaGremlin" even has a custom script language which allows operators to schedule custom tasks to be executed on the target machine.

"Assassin" is a similar kind of malware; it is an automated implant that provides a simple collection platform on remote computers running the Microsoft Windows operating system. Once the tool is installed on the target, the implant is run within a Windows service process. "Assassin" (just like "AfterMidnight") will then periodically beacon to its configured listening post(s) to request tasking and deliver results. Communication occurs over one or more transport protocols as configured before or during deployment. The "Assassin" C2 (Command and Control) and LP (Listening Post) subsystems are referred to collectively as "The Gibson" and allow operators to perform specific tasks on an infected target..


 [AlphaGremlin v0.1.0 Users Guide](#) [AfterMidnight Diagrams](#) [Assassin v1.4 Users Guide](#) [Assassin v1.3 Users Guide](#)[See more](#)

Archimedes

5 May, 2017

Today, May 5th 2017, WikiLeaks publishes "Archimedes", a tool used by the CIA to attack a computer inside a Local Area Network (LAN), usually used in offices. It allows the re-directing of traffic from the target computer inside the LAN through a computer infected with this malware and controlled by the CIA. This technique is used by the CIA to redirect the

Leaked Documents

 [Archimedes 1.0 User Guide](#) [Archimedes 1.3 Addendum](#)

machines to bring targeted computers under control and allowing further exploitation and abuse.



[Fulcrum User Manual
v0.62](#)

[See more](#)

Scribbles

28 April, 2017

Today, April 28th 2017, WikiLeaks publishes the documentation and source code for CIA's "Scribbles" project, a document-watermarking preprocessing system to embed "Web beacon"-style tags into documents that are likely to be copied by Insiders, Whistleblowers, Journalists or others. The released version (v1.0 RC1) is dated March, 1st 2016 and classified SECRET//ORCON/NOFORN until 2066.

Scribbles is intended for off-line preprocessing of Microsoft Office documents. For reasons of operational security the user guide demands that "[t]he Scribbles executable, parameter files, receipts and log files should not be installed on a target machine, nor left in a location where it might be collected by an adversary."

According to the documentation, "the Scribbles document watermarking tool has been successfully tested on [...] Microsoft Office 2013 (on Windows 8.1 x64), documents from Office versions 97-2016 (Office 95 documents will not work!) [and d]ocuments that are not be locked forms, encrypted, or password-protected". But this limitation to Microsoft Office documents seems to create problems: "If the targeted end-user opens them up in a different application, such as OpenOffice or LibreOffice, the watermark images and URLs may be visible to the end-user. For this reason, always make sure that the host names and URL components are logically consistent with the original content. If you are concerned that the targeted end-user may open these documents in a non-Microsoft Office application, please take some test documents and evaluate them in the likely application before deploying them."

Leaked Documents



[Scribbles v1.0 RC1 -
User Guide](#)



[Scribbles \(Source
Code\)](#)



[Scribbles v1.0 RC1 -
IVVRR Checklist](#)



[Scribbles v1.0 RC1 -
Readiness Review
Worksheet](#)

Weeping Angel

21 April, 2017

Today, April 21st 2017, WikiLeaks publishes the User Guide for CIA's "Weeping Angel" tool - an implant designed for Samsung F Series Smart Televisions. Based on the "Extending" tool from the MI5/BTSS, the implant is designed to record audio from the built-in microphone and egress or store the data.

The classification marks of the User Guide document hint that it was originally written by the British MI5/BTSS and later shared with the CIA. Both agencies collaborated on the further development of the malware and coordinated their work in Joint Development Workshops.

Leaked Documents



[Extending - User Guide](#)

Hive

14 April, 2017

Today, April 14th 2017, WikiLeaks publishes six documents from the CIA's [HIVE](#) project created by its "[Embedded Development Branch](#)" (EDB).

HIVE is a back-end infrastructure malware with a public-facing HTTPS interface which is used by CIA implants to transfer exfiltrated information from target machines to the CIA and to receive commands from its operators to execute specific tasks on the targets. HIVE is used across multiple malware implants and CIA operations. The public HTTPS interface utilizes unsuspicious-looking cover domains to hide its presence.

Anti-virus companies and forensic experts have noticed that some possible state-actor malware used such kind of back-end infrastructure by analyzing the communication behaviour of these specific implants, but were unable to attribute the back-end (and therefore the implant itself) to operations run by the CIA. In a recent [blog post by Symantec](#), that was able to attribute the "Longhorn" activities to the CIA based on the [Vault 7](#), such back-end infrastructure is described:

Leaked Documents



[Users Guide](#)



[Developers Guide](#)



[Developers Guide \(Figures\)](#)



[Hive Beacon Infrastructure](#)



[Hive Infrastructure Installation and Configuration Guide](#)

[See more](#)

legitimate companies offering virtual private server (VPS) or webhosting services. The malware communicates with C&C servers over HTTPS using a custom underlying cryptographic protocol to protect communications from identification.

The documents from this publication might further enable anti-malware researchers and forensic experts to analyse this kind of communication between malware implants and back-end servers used in previous illegal activities.

Grasshopper

7 April, 2017

Today, April 7th 2017, WikiLeaks releases Vault 7 "Grasshopper" -- 27 documents from the CIA's [Grasshopper framework](#), a platform used to build customized malware payloads for Microsoft Windows operating systems.

Grasshopper is provided with a variety of modules that can be used by a CIA operator as blocks to construct a customized implant that will behave differently, for example maintaining persistence on the computer differently, depending on what particular features or capabilities are selected in the process of building the bundle. Additionally, Grasshopper provides a very flexible language to define rules that are used to "perform a pre-installation survey of the target device, assuring that the payload will only [be] installed if the target has the right configuration". Through this grammar CIA operators are able to build from very simple to very complex logic used to determine, for example, if the target device is running a specific version of Microsoft Windows, or if a particular Antivirus product is running or not.

Grasshopper allows tools to be installed using a variety of persistence mechanisms and modified using a variety of extensions (like encryption).

The [requirement list](#) of the *Automated Implant Branch* (AIB) for Grasshopper puts special attention on [PSP avoidance](#), so that any *Personal Security Products* like 'MS Security Essentials', 'Rising',

Leaked Documents



Grasshopper-v1_1-AdminGuide



Grasshopper-v2_0_2-UserGuide



StolenGoods-2_1-UserGuide



GH-Module-Null-v2_0-UserGuide



GH-Module-Buffalo-Bamboo-v1_0-UserGuide

[See more](#)

Carberp, a suspected Russian organized crime rootkit." confirming the [recycling of malware](#) found on the Internet by the CIA. "The source of Carberp was published online, and has allowed AED/RDB to easily steal components as needed from the malware.". While the CIA claims that "[most] of Carberp was not used in Stolen Goods" they do acknowledge that "[the] persistence method, and parts of the installer, were taken and modified to fit our needs", providing a further example of reuse of portions of publicly available malware by the CIA, as observed in their [analysis of leaked material from the italian company "HackingTeam"](#).

The documents WikiLeaks publishes today provide an insights into the process of building modern espionage tools and insights into how the CIA maintains persistence over infected Microsoft Windows computers, providing directions for those seeking to defend their systems to identify any existing compromise

Marble Framework

31 March, 2017

Today, March 31st 2017, WikiLeaks releases [Vault 7 "Marble"](#) -- [676 source code files](#) for the CIA's secret anti-forensic [Marble Framework](#).

Marble is used to hamper forensic investigators and anti-virus companies from attributing viruses, trojans and hacking attacks to the CIA.

Marble does this by hiding ("obfuscating") text fragments used in [CIA malware](#) from visual inspection. This is the digital equivalent of a specialized CIA tool to place covers over the english language text on U.S. produced weapons systems before giving them to insurgents secretly backed by the CIA.

Marble forms part of the CIA's [anti-forensics approach](#) and the CIA's [Core Library](#) of malware code. It is "[D]esigned to allow for flexible and easy-to-use obfuscation" as "string obfuscation algorithms (especially those that are unique) are often used to link malware to a specific developer or development shop."

Leaked Documents



[Marble Framework](#)
(Source Code)

use at the CIA during 2016. It reached 1.0 in 2015.

The source code shows that Marble has test examples not just in English but also in Chinese, Russian, Korean, Arabic and Farsi. This would permit a forensic attribution double game, for example by pretending that the spoken language of the malware creator was not American English, but Chinese, but then showing attempts to conceal the use of Chinese, drawing forensic investigators even more strongly to the wrong conclusion, --- but there are other possibilities, such as hiding fake error messages.

The Marble Framework is used for obfuscation only and does not contain any vulnerabilities or exploits by itself.

Dark Matter

23 March, 2017

Today, March 23rd 2017, WikiLeaks releases Vault 7 "Dark Matter", which contains documentation for several CIA projects that infect Apple Mac firmware (meaning the infection persists even if the operating system is re-installed) developed by the CIA's Embedded Development Branch (EDB). These documents explain the techniques used by CIA to gain 'persistence' on Apple Mac devices, including Macs and iPhones and demonstrate their use of EFI/UEFI and firmware malware.

Among others, these documents reveal the "Sonic Screwdriver" project which, as explained by the CIA, is a "mechanism for executing code on peripheral devices while a Mac laptop or desktop is booting" allowing an attacker to boot its attack software for example from a USB stick "even when a firmware password is enabled". The CIA's "Sonic Screwdriver" infector is stored on the modified firmware of an Apple Thunderbolt-to-Ethernet adapter.

"DarkSeaSkies" is "an implant that persists in the EFI firmware of an Apple MacBook Air computer" and consists of "DarkMatter", "SeaPea" and "NightSkies", respectively EFI, kernel-space and user-space implants.

Leaked Documents

[Sonic Screwdriver](#)[DerStarke v1.4](#)[DerStarke v1.4 RC1 - IVVRR Checklist](#)[DarkSeaSkies v1.0 - Test Plan Procedures](#)[FDOS_1_0_FINAL_freedos_setup](#)[See more](#)

these systems and is working on the production of [DerStärke2.0](#).

Also included in this release is the manual for the CIA's "NightSkies 1.2" a "beacon/loader/implant tool" for the Apple iPhone. Noteworthy is that NightSkies had reached 1.2 by 2008, and is expressly designed to be physically installed onto factory fresh iPhones. i.e the CIA has been infecting the iPhone supply chain of its targets since at least 2008.

While CIA assets are sometimes used to physically infect systems in the custody of a target it is likely that many CIA physical access attacks have infected the targeted organization's supply chain including by interdicting mail orders and other shipments (opening, infecting, and resending) leaving the United States or otherwise.

Media Partners

DER SPIEGEL - Germany

LA REPUBBLICA - Italy

LIBERATION - France

MEDIAPART - France

Expert Organizations

↑
Top



WL Research
Community - user
contributed research
based on documents



Tor is an encrypted
anonymising network
that makes it harder
to intercept internet
communications, or



Tails is a live
operating system, that
you can start on
almost any computer
from a DVD, USB



The Courage
Foundation is an
international
organisation that
supports those who

Bitcoin uses peer-to-
peer technology to
operate with no
central authority or
banks; managing